Journal of Pure and Applied Algebra 215 (2011) 2666–2673

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

Zariski surfaces, class groups and linearized systems

Jeffrey Lang

Mathematics Department, University of Kansas, Lawrence, KS, 66045, USA

ARTICLE INFO

Article history:
Received 17 September 2010
Received in revised form 17 January 2011
Available online 27 March 2011
Communicated by S. Iyengar

MSC: 13A99

ABSTRACT

Galois descent and linearized systems in characteristic $p \neq 0$ are applied to the study of divisor class groups of Zariski surfaces. An efficient method is obtained for calculating their class groups and, for a general case, an easily calculated matrix is defined whose rank determines the class group order.

0. Introduction

Let k be an algebraically closed field of characteristic $p \neq 0$ and $X_g \subset \mathbb{A}^3_k$ a normal surface defined by an equation of the form $z^p = g(x, y)$ with $g \in k[x, y]$. Varieties of this type are known as Zariski surfaces and much effort has been focused on understanding their divisor class groups. The class group could often be an elusive invariant, but apparent breakthroughs for Zariski surfaces came in [1,2] and [4] which present programmable algorithms for calculating them. However, recently I discovered errors in both of them. The algorithm developed in [1] depends on an incorrect lemma (Lemma 5, p. 249). It can be corrected, but the program is already too slow to make it worth the effort, as the program often takes several hours to complete the computation, even for cases of low degree and small characteristic. The algorithm in [4] is more efficient than the original one, but it contains a computational ambiguity that requires a considerably more complex program to correct (Step 5 of the algorithm, pp. 5–6, and [6]). This paper presents a new algorithm for computing the class group of a Zariski surface. It is much simpler and computationally more efficient than earlier algorithms, particularly in the general case discussed in Section 4. Unlike its predecessors, it does not require calculating pth roots, avoids lengthy loops, and involves only standard matrix computations already built into most mathematical programs. Perhaps most importantly, in Section 4, for a general case, it defines an easily calculated matrix whose rank completely determines the order of the class group of X_g, which should shed light on how class group order stratifies the moduli space of Zariski surfaces in each characteristic.

1. Preliminaries

The algorithms derived in this article is based on Galois descent techniques developed in Pierre Samuel's Tata notes [7]. The reader is referred there for the definitions of a Krull domain and divisor class group of a Krull domain [7, pp. 1–4]. All of the rings studied herein are Noetherian integrally closed domains and are thus Krull rings [7, p. 6]. If R is a Noetherian integrally closed domain, then $X = Spec(R)$ is regular in codimension one and the group of Weil divisors of X, denoted $Cl(X)$, and the divisor class group of R, denoted $Cl(R)$, as defined by Samuel are isomorphic [3, p. 130]. The following theorems are from Samuel's notes.

Theorem 1.1. *Let $A \subset B$ be Krull rings with B integral over A. Then there is a well defined group homomorphism $\phi : Cl(A) \to Cl(B)$ [7, pp. 19–20].*

Remark 1.2. The homomorphism $\phi : Cl(A) \to Cl(B)$ can be described by its behavior on height one prime ideals, since their divisors generate the class group of a Krull domain [7, pp. 5–7]. If Q is a height one prime of A, then $\phi(Q) = \sum e(q : Q)q$,

E-mail address: lang@math.ku.edu.

0022-4049/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2011.03.011

where the sum is over all prime ideals q lying over Q (which are necessarily height one) and $e(q : Q)$ is the ramification index of q over Q [7, pp. 18–21].

Remark 1.3. Let B be a Krull ring of characteristic $p \neq 0$ and L be the quotient field of B. Let $\triangle$ be a derivation of L such that $\triangle(B) \subset B$. Let $K =$ kernel of $\triangle$ and $A = B \bigcap K$. Then A is a Krull ring with B integral over A (since $B^p \subset A$). Set $\mathscr{L} = \{a^{-1}\triangle a : a \in L \text{ and } a^{-1}\triangle a \in B\}$ and $\mathscr{L}' = \{u^{-1}\triangle u : u \text{ is a unit in } B\}$. Then $\mathscr{L}'$ is an additive subgroup of $\mathscr{L}$.

Theorem 1.4. (a) *Let $\phi : Cl(A) \to Cl(B)$ be the homomorphism described in (1.2). There exists a canonical monomorphism $\bar{\phi} : ker\phi \to \mathscr{L}/\mathscr{L}'$.* (b) *If L is the quotient field of B and $[L : K] = p$ and $\triangle(B)$ is not contained in any height one prime of B, then $\bar{\phi}$ is an isomorphism [7, pp. 63–64].*

Remark 1.5. If $I \in Cl(A)$ is in the $ker\phi$, then $\phi(I) = aB$ for some $a \in L$. Samuel shows that $a^{-1}\triangle a \in B$ and defines $\bar{\phi}(I) = a^{-1}\triangle a$. Since $\mathscr{L} \subset B$ and the characteristic of L is p, each nonzero element of $ker\phi$ has order p.

Theorem 1.6. *If $[L : K] = p$, then* (a) *there exists $\alpha \in A$ such that $\triangle^p = \alpha\triangle$ and* (b) *an element $t \in L$ is equal to $v^{-1}\triangle v$ for some $v \in L$ if and only if $\triangle^{p-1}t - \alpha t + t^p = 0$ [7, pp. 63–64].*

2. Galois descent and logarithmic derivatives

Hereafter, k represents an algebraically closed field of characteristic $p \neq 0$ and $g \in k[x, y]$ a polynomial of degree $n \neq 0$ such that g_x and g_y have no common factors in $k[x, y]$. X_g will denote the surface in A^3_k defined by the equation $z^p = g$ and D_g the Jacobian derivation on $k(x, y)$ defined by $D_g = g_y\frac{\partial}{\partial x} - g_x\frac{\partial}{\partial y}$. F_g will denote the field extension of the prime subfield generated by the coefficients of g.

Lemma 2.1. *The coordinate ring of X_g is isomorphic to the ring $B_g = k[x^p, y^p, g]$.*

Proof. Let $\theta : k[x, y, z] \to B_g$ be the homomorphism that sends x to x^p, y to y^p, z to g, and a to a^p for all $a \in k$. θ is surjective since k is perfect. Hence, $ker\theta$ is a height one prime ideal containing the principal ideal I generated by $z^p - g$. Since the latter is a height one prime, $I = ker\theta$. Therefore, the coordinate ring of X_g is isomorphic to B_g. □

Lemma 2.2. $B_g = D_g^{-1}(0) \cap k[x, y]$.

Proof. Since $D_g(x) = g_y \neq 0$, $k(x^p, y^p) \subsetneq k(x^p, y^p, g) \subset D_g^{-1}(0) \subsetneq k(x, y)$. Hence, $k(x^p, y^p, g) = D_g^{-1}(0)$. Since X_g has only finitely many singular points, B_g is normal by (2.1) and Serre's normality criterion. Since $D_g^{-1}(0) \cap k[x, y]$ is integral over B_g and they have the same quotient field, the two are equal. □

Lemma 2.3. *Let $\mathscr{L}_g = \{f^{-1}D_g f : f \in k(x, y) \text{ and } f^{-1}D_g f \in k[x, y]\}$ be the additive group of logarithmic derivatives of D_g in $k[x, y]$. Then $Cl(B_g) \cong \mathscr{L}_g$.*

Proof. By (1.4) and the fact that $D_g(k[x, y])$ is not contained in any height one prime of $k[x, y]$ (since $D_g(x) = g_y$ and $D_g(y) = -g_x$) and $[k(x, y) : k(x^p, y^p, g)] = p$. □

Remark 2.4. By (1.6) there exists $\alpha_g \in B_g$ such that $D_g^p = \alpha_g D_g$. In 1980, Richard Ganong conjectured to me that α_g is given by the formula, $\alpha_g = \sum_{i=0}^{p-1} g^i\nabla(g^{p-1-i})$, where $\nabla = \partial^{2p-2}/\partial x^{p-1}\partial y^{p-1}$. In an attempt to verify this, the author proved the next theorem [5] under the assumption that the highest degree form of g is not in $k[x^p, y^p]$. Stohr and Voloch later proved it in general [8].

Theorem 2.5. *Let $\alpha_g \in B_g$ be such that $D_g^p = \alpha_g D_g$. Then for all $f \in k[x, y]$, $D_g^{p-1}f - \alpha_g f = -\sum_{i=0}^{p-1} g^i\nabla(g^{p-1-i}f)$, where $\nabla = \partial^{2p-2}/\partial x^{p-1}\partial y^{p-1}$.*

Corollary 2.6. $\alpha_g = \sum_{i=0}^{p-1} g^i\nabla(g^{p-1-i})$.

Proof. Let $f = 1$ in (2.5). □

Corollary 2.7. *A polynomial $t \in k[x, y]$ is in $\mathscr{L}_g$ if and only if $\nabla(g^i t) = 0$, for $i = 0, 1, \ldots, p-2$, and $\nabla(g^{p-1}t) = t^p$.*

Proof. Since $\nabla(k(x, y)) = k(x^p, y^p)$ and $\{g^i : 0 \leqq i \leqq p-1\}$ is independent over $k(x^p, y^p)$, the corollary follows by (1.6) and (2.5). □

Proposition 2.8. *Let $\mathscr{H}_g = \{t \in k[x, y] : \nabla(g^{p-1}t) = t^p\}$. Then $\mathscr{L}_g \subset \mathscr{H}_g$ and $deg(t) \leq n - 2$ for each $t \in \mathscr{H}_g$.*

Proof. $\mathscr{L}_g \subset \mathscr{H}_g$ by (2.7). A comparison of degrees on both sides of the equation $\nabla(g^{p-1}t) = t^p$ yields $pdeg(t) \leq deg(t) + (p-1)n - 2(p-1)$, i.e. $deg(t) \leq n - 2$. □

Definition 2.9. For a field F and positive integers r and s , let $F^{r\times s}$ be the set of $r \times s$ matrices with entries in F. If $M = [a_{ij}] \in F^{r\times s}$ and q is an integer, let $M^{(p^q)} = [a_{ij}^{p^q}]$. I_r will denote the identity matrix in $F^{r\times r}$ and 0_{rs} the zero matrix in $F^{r\times s}$. When the context makes plain the dimension of the zero matrix, we will simply denote it by 0. If $M \in F^{r\times s}$, let $row(M)$ denote the row space of M.

Definition 2.10. Let $g \in k[x, y]$ be as above. Let V be the k-vector space of polynomials in $k[x, y]$ of degree at most $n-2$ (where $n = deg(g)$) and for each $r = 0, \ldots, p-1$, let W_r be the k-vector space of polynomials in $k[x^p, y^p]$ of degree at most $(r+1)n - 2p$. For $r = 0, \ldots, p-1$, let $T_r : V \to W_r$ be the linear transformation defined by $T_r(f) = \nabla(g^r f)$ and let $M_{g,r}$ be the matrix of T_r with respect to the monomial bases $\{x^i y^j : 0 \le i+j \le n-2\}$ and $\{x^{ip} y^{jp} : 0 \le i+j \le \frac{(r+1)n}{p} - 2\}$ of V and W_r, respectively. Then $M_{g,r}$ is a $\frac{n_r(n_r-1)}{2} \times \frac{n(n-1)}{2}$ matrix with coefficients in k, where n_r is the greatest integer less than or equal to $\frac{(r+1)n}{p}$.

Lemma 2.11. *For each $t = \sum_{i+j=0}^{n-2} \alpha_{ij} x^i y^j \in k[x, y]$, let $\vec{x}_t = \begin{bmatrix} \alpha_{00} \\ \alpha_{10} \\ \alpha_{01} \\ \vdots \end{bmatrix}$ in $k^{\frac{n(n-1)}{2}}$. Then the map $t \to \vec{x}_t$ maps $\mathscr{H}_g$ isomorphically to the group of solutions of the square system $M_{g,p-1}\vec{x} = \vec{x}^{(p)}$, with $\vec{x}^{(p)}$ as in (2.9), and maps $\mathscr{L}_g$ isomorphically to the group of solutions of the system $M_{g,i}\vec{x} = \vec{0}$, $0 \le i \le p-2$, $M_{g,p-1}\vec{x} = \vec{x}^{(p)}$.*

Proof. The system $M_{g,p-1}\vec{x} = \vec{x}^{(p)}$ is obtained by comparing coefficients on both sides of the equality $\nabla(g^{p-1}t) = t^p$. Thus t is a solution of the latter equation if and only if $\vec{x}_t$ is a solution of the matrix equation. The map is also clearly additive. Similarly, the system $M_{g,i}\vec{x} = \vec{0}$, $0 \le i \le p-2$, $M_{g,p-1}\vec{x} = \vec{x}^{(p)}$ is obtained by comparing coefficients on both sides of the equations $\nabla(g^i t) = 0$, for $i = 0, 1, \ldots, p-2$, and $\nabla(g^{p-1}t) = t^p$ in (2.7). □

Definition 2.12. By (2.10), $M_{g,p-1}$ is a square matrix of dimension $\frac{n(n-1)}{2}$, which hereafter will be denoted simply by M_g. Also, let L_g denote the block matrix $\begin{bmatrix} M_{g,0} \\ \vdots \\ M_{g,p-2} \end{bmatrix}$. By (2.11), $t \to \vec{x}_t$ maps $\mathscr{L}_g$ isomorphically to the group of solutions of the system $L_g\vec{x} = \vec{0}$, $M_g\vec{x} = \vec{x}^{(p)}$.

3. Linearized systems

Definition 3.1. Let $A \in k^{rxr}$ and $L \in k^{s\times r}$. Let $\pi : k^{r+s} \to k^r$ be the projection $\pi_r \begin{bmatrix} a_1 & \cdots & a_{r+s} \end{bmatrix} = \begin{bmatrix} a_1 & \cdots & a_r \end{bmatrix}$. Given $\mathscr{B}_0 = \{\vec{y}_1, \ldots, \vec{y}_m\}$ a basis of the left orthogonal complement of the block matrix $\begin{bmatrix} A \\ L \end{bmatrix}$, let $L^{(A,\mathscr{B}_0)} \in k^{(s+m)\times r}$ be defined by $L^{(A,\mathscr{B}_0)} = \begin{bmatrix} L \\ [\mathscr{B}_0]^{(\frac{1}{p})} \end{bmatrix}$, where $[\mathscr{B}_0] = \begin{bmatrix} \pi(\vec{y}_1) \\ \vdots \\ \pi(\vec{y}_m) \end{bmatrix}$ in $k^{m\times r}$. Now let $L_0 = L$ and for each $i = 0, 1, \ldots$, let $L_{i+1} = L_i^{(A,\mathscr{B}_i)}$, where $\mathscr{B}_i$ is a basis for the left orthogonal complement of $\begin{bmatrix} A \\ L_i \end{bmatrix}$.

Lemma 3.2. *Let $A \in k^{r\times r}$, $L \in k^{s\times r}$, W be the left orthogonal complement of $\begin{bmatrix} A \\ L \end{bmatrix}$, and $\vec{v} \in k^{1\times r}$. Then $\vec{v} \in \pi_r(W)$ if and only if $\vec{v}A \in row(L)$.*

Proof. $\vec{v} = \pi_r(\vec{w})$ for some $\vec{w} = [a_1, \ldots, a_{r+s}] \in W$ if and only if $\vec{v}A = -[a_{r+1}, \ldots, a_{r+s}]L \in row(L)$. □

Notation 3.3. Let A in $k^{r\times r}$, L in $k^{s\times r}$, and L_i be as defined in (3.1). For each i, let $r_i(A, L) = rank(L_i)$ and $r(A, L) = r_{i_0}(A, L)$, where i_0 is minimal such that $r_{i_0}(A, L) = r_{i_0+1}(A, L)$.

Remark 3.4. $r_i(A, L)$, i_0, and $r(A, L)$ in (3.3) do not depend on the choices of bases of the orthogonal complements at each step in (3.1). Also, $i_0 \le r - rank(L)$ since for each i, L_i is a submatrix of L_{i+1}.

Lemma 3.5. *Let $A \in k^{r\times r}$, $L \in k^{s\times r}$ and i_0 be minimal such that $r_{i_0}(A, L) = r_{i_0+1}(A, L)$. Then $r(A, L) = r_i(A, L)$ for all $i \ge i_0$.*

Proof. Suppose $r_j(A, L) = r_{j+1}(A, L)$ for some positive integer j. Then $row(L_j) = row(L_{j+1})$. Thus if some linear combination of the rows of A belongs to $row(L_{j+1})$, then the same combination of the rows of A belongs to $row(L_j)$, and vice versa. From this it follows that if W_j and W_{j+1} are the left orthogonal complements of $\begin{bmatrix} A \\ L_j \end{bmatrix}$ and $\begin{bmatrix} A \\ L_{j+1} \end{bmatrix}$, respectively, then $\pi_r(W_j) = \pi_r(W_{j+1})$. Therefore, $row(L_{j+1}) = row(L_{j+2})$, i.e. $r_{j+1}(A, L) = r_{j+2}(A, L)$. □

Lemma 3.6. *Let $A \in k^{r\times r}$, $L \in k^{s\times r}$, and $\mathscr{B} = \{\vec{y}_1, \ldots, \vec{y}_m\}$ be a basis of the left orthogonal complement of $\begin{bmatrix} A \\ L \end{bmatrix}$. Then the solution set of the system $A\vec{x} = \vec{x}^{(p)}$, $L\vec{x} = \vec{0}$, is identical to the solution set of the system $A\vec{x} = \vec{x}^{(p)}$, $L_1\vec{x} = \vec{0}$, where $L_1 = L^{(A,\mathscr{B})}$.*

Proof. Since L is a submatrix of L_1, the solution set of the second system is contained in that of the first. If $\vec{y} = \begin{bmatrix} a_1 & \cdots & a_r & b_1 & \cdots & b_s \end{bmatrix}$ is in the left orthogonal complement of $\begin{bmatrix} A \\ L \end{bmatrix}$, then $\ell = a_1\ell_1 + \cdots + a_r\ell_r \in row(L)$. Hence, if $(x_1, \ldots, x_r)$ is a solution of the system $L\vec{x} = \vec{0}$, then $\ell\vec{x} = \vec{0}$. Hence, if $(x_1, \ldots, x_r)$ is a solution of the system, $A\vec{x} = \vec{x}^{(p)}$, $L\vec{x} = \vec{0}$, then $\vec{0} = \ell\vec{x} = [a_1 \cdots a_r]A\vec{x} = [a_1 \cdots a_r]\vec{x}^{(p)} = a_1x_1^p + \cdots + a_rx_r^p$, and therefore $(x_1, \ldots, x_r)$ is a solution of the linear equation corresponding to the matrix $\begin{bmatrix} a_1^{\frac{1}{p}} & \cdots & a_r^{\frac{1}{p}} \end{bmatrix} = \pi(\vec{y})^{(\frac{1}{p})}$. Therefore, the solution set of $A\vec{x} = \vec{x}^{(p)}$, $L\vec{x} = \vec{0}$ is contained in that of $A\vec{x} = \vec{x}^{(p)}$, $L_1\vec{x} = \vec{0}$. □

Proposition 3.7. *Let $A \in k^{r\times r}$, $L \in k^{s\times r}$, L_i $(i = 0, 1, 2, \ldots)$ be as in (3.1). Assume i_0 is the minimum i such that $r_i(A, L) = r_{i+1}(A, L)$. Then rank $\left(\begin{bmatrix} A \\ L_{i_0} \end{bmatrix}\right) = r$.*

Proof. We proceed by induction on the number of nonzero columns of A. If A has no nonzero columns, then A is the zero matrix and $L_1 = I_r$. If the $rank(L_0) = r$, then $i_0 = 0$ and $rank\begin{pmatrix} A \\ L_0 \end{pmatrix} = r$. If $rank(L_0) < r$, then $i_0 = 1$ and $rank\left(\begin{bmatrix} A \\ L_1 \end{bmatrix}\right) = r$.

Assume now that A has exactly s nonzero columns, which after a permutation of columns we may assume are the first s columns of A, counting from the left. Thus $A = \begin{bmatrix} A' & 0_{r(r-s)} \end{bmatrix}$, with $A' \in k^{r\times s}$. If $t = rank(A)$, then $t \le s$. Without loss of generality we may assume that the top t rows of A are a basis of $row(A)$. Then each of the last $r - t$ rows of A are linear combinations of the first t rows. This implies by (3.2) that the left orthogonal complement of A has a basis $\mathscr{B}$ consisting of elements of the form $\vec{w}_i = \begin{bmatrix} b_{i1} & \cdots & b_{is} & 0 & \cdots & 0 \end{bmatrix} + \vec{e}_i$, $t + 1 \le i \le r$, where $\vec{e}_i \in k^{1\times r}$ has 1 in the ith position and 0 elsewhere. Since the left orthogonal complement of A is contained in the left orthogonal complement of $\begin{bmatrix} A \\ L \end{bmatrix}$, $\mathscr{B}$ can be extended to a basis $\mathscr{B}_0$ of the left orthogonal complement of $\begin{bmatrix} A \\ L \end{bmatrix}$. Hence, $L_1 = L^{(A,\mathscr{B}_0)}$ includes rows of the same form, i.e. L_1 contains a submatrix of the form $\begin{bmatrix} L' & I_{r-t} \end{bmatrix}$, where $L' \in k^{(r-t)\times t}$. Using elementary row operations, we can eliminate all entries in A above I_{r-t} in $\begin{bmatrix} A \\ L_1 \end{bmatrix}$ by subtracting from each row of A an element of $row\left(\begin{bmatrix} L' & I_{r-t} \end{bmatrix}\right)$, thus replacing A in $\begin{bmatrix} A \\ L_1 \end{bmatrix}$ by a row-equivalent matrix $B = \begin{bmatrix} A'' & 0_{r(r-t)} \end{bmatrix}$, with $A'' \in k^{r\times t}$, and by (3.2) having the property that π_r of the left orthogonal complement of $\begin{bmatrix} A \\ L_1 \end{bmatrix}$ is equal to π_r of the left orthogonal complement of $\begin{bmatrix} B \\ L_1 \end{bmatrix}$.

We now distinguish between two cases.

Case 1. If $t = s$, then $rank\left(\begin{bmatrix} A \\ L_1 \end{bmatrix}\right) = r$ and $rank\left(\begin{bmatrix} A \\ L_i \end{bmatrix}\right) = r$ for all $i \ge 1$, which agrees with the statement of the proposition if $i_0 \ge 1$. If $i_0 = 0$, then $row(L_0) = row(L_i)$ for all $i \ge 0$, which implies $rank\left(\begin{bmatrix} A \\ L_0 \end{bmatrix}\right) = rank\left(\begin{bmatrix} A \\ L_1 \end{bmatrix}\right) = r$, which verifies the proposition.

Case 2. If $t < s$, then by induction, the statement of the theorem holds for B and L_1 and hence for A and L_1. Then if $i_0 \ge 1$, the minimal i such that $r_i(A, L_1) = r_{i+1}(A, L_1)$ is $i_0 - 1$, from which we obtain $rank\left(\begin{bmatrix} A \\ L_{i_0} \end{bmatrix}\right) = r$. If $i_0 = 0$, then again $row(L_0) = row(L_i)$ for all $i \ge 0$ and $rank\left(\begin{bmatrix} A \\ L_0 \end{bmatrix}\right) = rank\left(\begin{bmatrix} A \\ L_1 \end{bmatrix}\right) = r$, since the theorem holds for A and L_1 and the minimal i such that $r_i(A, L_1) = r_{i+1}(A, L_1)$ is 0, which verifies the proposition. □

Corollary 3.8. *Let $A \in k^{r\times r}$, $L \in k^{s\times r}$, L_i $(i = 0, 1, 2, \ldots)$ be as in (3.1). Assume $j \in \mathbb{N}$ such that $r_j(A, L) = r_{j+1}(A, L)$. Then $rank\left(\begin{bmatrix} A \\ L_j \end{bmatrix}\right) = r$.*

Proof. By (3.7) and the fact that $row(L_i) = row(L_{i+1})$ for all i. □

Lemma 3.9. *Let $B \in k^{r\times r}$ and assume $det(B) \neq 0$. Then the solution set of the system $B\begin{bmatrix}\vec{x}\\ \vec{y}\end{bmatrix} = \begin{bmatrix}\vec{x}^{(p)}\\ \vec{0}\end{bmatrix}$ with $\vec{x}$ in k^s and $\vec{y}$ in k^{r-s} is a p-group of type $(p,\dots,p)$ of order p^s.*

Proof. By Bezout's theorem the system has p^s solutions, counted with multiplicity and considered in projective space. Clearly, there are no solutions at infinity. If $(a_1,\dots,a_r)$ is a solution of $B\begin{bmatrix}\vec{x}\\ \vec{y}\end{bmatrix} = \begin{bmatrix}\vec{x}^{(p)}\\ \vec{0}\end{bmatrix}$, then the system remains fixed under the change of coordinates $x_i \to x_i - a_i$. Hence, every solution has the same multiplicity, which is one since $det(B) \neq 0$. The other conclusions are simple consequences of the fact that $char(k) = p$. □

Theorem 3.10. *Let $A \in k^{r\times r}$, $L \in k^{s\times r}$. Then the system $A\vec{x} = \vec{x}^{(p)}$, $L\vec{x} = \vec{0}$ is a p-group of type $(p,\dots,p)$ of order $p^{r-r(A,L)}$.*

Proof. Let L_i, $i = 0, 1, 2, \dots,$ be as described in (3.1) and let $m = r(A, L)$. Let j be any positive integer such that $r_j(A, L) = r_{j+1}(A, L)$. By (3.5) $rank(L_j) = r_j(A, L) = m$. By (3.6) the solution set of the system $A\vec{x} = \vec{x}^{(p)}$, $L\vec{x} = \vec{0}$ is identical to the solution set of the system $A\vec{x} = \vec{x}^{(p)}$, $L_j\vec{x} = \vec{0}$. By (3.8) $rank\left(\begin{bmatrix}A\\ L_j\end{bmatrix}\right) = r$. Hence, there are submatrices $A' \in k^{(r-m)\times r}$ of A and $L_j' \in k^{m\times r}$ of L_j such that $rank\left(\begin{bmatrix}A'\\ L_j'\end{bmatrix}\right) = r$. The solution set of $A\vec{x} = \vec{x}^{(p)}$, $L_j\vec{x} = \vec{0}$ is contained in the solution set of the system $A'\vec{x} = \vec{x}^{(p)}$, $L_j'\vec{x} = \vec{0}$.

To show the reverse containment, it is enough to show that if $I, I' \subset k[x_1,\dots,x_r]$ are the ideals generated by the polynomials defining the first and second system, respectively, then $I \subset I'$. Without loss of generality, we may assume A' consists of the top $r - m$ rows of A. Since $rank(L_j') = rank(L_j)$, we need only show that the polynomials corresponding to the last m equations of $A\vec{x} = \vec{x}^{(p)}$ belong to I'. Let $\sum \alpha_{qi}x_i - x_q^p$, with $r - m < q \leq r$, be such a polynomial and $\vec{\alpha} = \begin{bmatrix}\alpha_{q1} & \cdots & \alpha_{qr}\end{bmatrix}$. Since $rank\left(\begin{bmatrix}A'\\ L_j'\end{bmatrix}\right) = r$, there exists a vector $\vec{a} = \begin{bmatrix}a_1 & \cdots & a_{r-m} & 0 & \cdots & 0\end{bmatrix} \in k^{1\times r}$ such that $\vec{a}A + \vec{\alpha} \in row(L_j') = row(L_j)$. Thus, $\sum \alpha_{qi}x_i + x_q^p \in I'$ if and only if $a_1x_1^p + \cdots + a_{r-m}x_{r-m}^p + x_q^p \in I'$, but by (3.2) the latter is the case since $\vec{a}^{(\frac{1}{p})} + \vec{e}_q \in row(L_{j+1}) = row(L_j)$, where $\vec{e}_q \in k^{1\times r}$ has 1 for the qth entry and all other entries 0.

Therefore, $A\vec{x} = \vec{x}^{(p)}$, $L\vec{x} = \vec{0}$ has the same solution group as $A'\vec{x} = \vec{x}^{(p)}$, $L_j'\vec{x} = \vec{0}$, which is a p-group of type $(p,\dots,p)$ of order p^{r-m} by (3.9). □

The determination of $r(A, L)$ involves repeated calculation of pth roots of increasing exponent. The next Proposition 3.12 shows that this can be avoided.

Definition 3.11. Let $A \in k^{r\times r}$ and let $L \in k^{s\times r}$. Let $\pi_r : k^{r+s} \to k^r$ be the projection $\pi_r\begin{bmatrix}a_1 & \cdots & a_{r+s}\end{bmatrix} = \begin{bmatrix}a_1 & \cdots & a_r\end{bmatrix}$. Given $\overline{\mathscr{B}} = \{\vec{y}_1,\dots,\vec{y}_m\}$ a basis of the left orthogonal complement of the block matrix $\begin{bmatrix}A\\ L\end{bmatrix}$, let $L^{[A,\overline{\mathscr{B}}]} \in k^{(s+m)\times r}$ be defined by $L^{[A,\overline{\mathscr{B}}]} = \begin{bmatrix}L^{(p)}\\ [\overline{\mathscr{B}}]\end{bmatrix}$, where $[\overline{\mathscr{B}}] = \begin{bmatrix}\pi(\vec{y}_1)\\ \vdots\\ \pi(\vec{y}_m)\end{bmatrix}$ in $k^{m\times r}$. Now let $\bar{L}_0 = L^{(p)}$ and for each $i = 0, 1, \dots,$ let $\bar{L}_{i+1} = \bar{L}_i^{[A_{i+1},\overline{\mathscr{B}}_i]}$, where $A_i = A^{(p^i)}$ and $\overline{\mathscr{B}}_i$ is a basis for the left orthogonal complement of $\begin{bmatrix}A_{i+1}\\ \bar{L}_i\end{bmatrix}$. For each i, let $r_i[A, L] = rank(\bar{L}_i)$ and $r[A, L] = r_{i_0}[A, L]$, where i_0 is minimal such that $r_{i_0}[A, L] = r_{i_0+1}[A, L]$. The next result implies that $r(A, L) = r[A, L]$.

Proposition 3.12. *Let $A \in k^{r\times r}$, $L \in k^{s\times r}$ and let L_i, $\mathscr{B}_i$, $\bar{L}_i$, $\overline{\mathscr{B}}_i$ be as described in (3.1) and (3.11), respectively. Then for each $i \geq 1$, $row(\bar{L}_i) = row(L_i^{(p^{i+1})})$.*

Proof. The $i = 0$ case is immediate from the definitions. Assume that for some positive integer j the statement of the proposition holds for all $i \leq j$. If $\mathscr{B}_j = \{\vec{y}_1,\dots,\vec{y}_m\}$ is a basis for the left orthogonal complement of $\begin{bmatrix}A\\ L_j\end{bmatrix}$, then $\mathscr{B}_j' = \{\vec{y}_1^{(p^{j+1})},\dots,\vec{y}_m^{(p^{j+1})}\}$ is a basis for the left orthogonal complement of $\begin{bmatrix}A^{(p^{j+1})}\\ L_j^{(p^{j+1})}\end{bmatrix}$, which by (3.2) has the same image

under π_r as the left orthogonal complement of $\begin{bmatrix} A^{(p^{j+1})} \\ \bar{L}_j \end{bmatrix} = \begin{bmatrix} A_{j+1} \\ \bar{L}_j \end{bmatrix}$ (since $row(\bar{L}_j) = row(L_j^{(p^{j+1})})$). Thus $row(\bar{L}_{j+1}) = row\left(\begin{bmatrix} \bar{L}_j^{(p)} \\ [\mathscr{B}'_j] \end{bmatrix}\right) = row\left(\begin{bmatrix} L_j^{(p^{j+2})} \\ [\mathscr{B}_j]^{(p^{j+1})} \end{bmatrix}\right) = row(L_j^{(p^{j+2})})$. □

Corollary 3.13. *Let $A \in k^{r\times r}$ and $L \in k^{s\times r}$. Then for each $i = 0, 1, 2, \ldots, r_i(A, L) = r_i[A, L]$. In particular, $r(A, L) = r[A, L]$.*

The Main Algorithm 3.14. Let $g \in k[x, y]$ be a polynomial of degree $n \neq 0$ such that g_x and g_y have no common factors in $k[x, y]$ and X_g the surface in A_k^3 defined by the equation $z^p = g$. Let $m = \frac{n(n-1)}{2}$. The determination of the group of Weil divisors of X_g reduces to the following series of standard matrix computations. Step (1) Determine $M_g \in k^{m\times m}$ and L_g as defined in (2.11) and (2.12). Step (2) Let $N = m - rank(L_g)$, $\bar{L}_0 = L_g^{(p)}$, and for each $1 \leq i \leq N$, calculate $\bar{L}_{i+1} = \bar{L}_i^{[A_{i+1}, \overline{\mathscr{B}_i}]}$ as described in (3.11), where $A_i = M_g^{(p^i)}$ and $\overline{\mathscr{B}_i}$ is a basis for the left orthogonal complement of $\begin{bmatrix} A_{i+1} \\ \bar{L}_i \end{bmatrix}$ $\left(\text{equivalently, } \overline{\mathscr{B}_i} \text{ is a basis for the kernel of } \begin{bmatrix} A_{i+1} \\ \bar{L}_i \end{bmatrix}^T\right)$. Step (3) By (3.4), (3.5), (3.10) and (3.13), $Cl(X_g)$ is a p-group of type $(p, \ldots, p)$ of order $p^{m-rank(\bar{L}_N)}$.

Remark 3.15 (*Modifications to the Main Algorithm*)**.** In (3.14) we calculate L_i until $i = N$ because (3.4) and (3.5) guarantee that $r(A, L) = rank(L_N)$ (i.e. $rank(L_N) = rank(L_{N+1})$). Alternatively, in Step 2, we could recursively calculate each L_i together with its rank until we determine i_0, the minimal i such that $rank(L_i) = rank(L_{i+1})$, in which case the order of $Cl(X_g)$ will be $p^{m-rank(L_{i_0})}$. Another option, which may be useful when n is large, is to replace each matrix $\bar{L}_i$ when it is calculated by its reduced row-echelon form. Lastly, note that when $g \in \mathbb{F}_p[x, y]$, then $M_g \in \mathbb{F}_p^{m\times m}$, where $\mathbb{F}_p$ is the prime subfield of k, and thus $A_i = M_g$ for each i.

4. The nonsingular case

This section considers the case where M_g is nonsingular, where M_g is as in Definition 2.12, and obtains a simplified version of the above algorithm (3.15).

Lemma 4.1. *Let $A \in k^{r\times r}$ be nonsingular and let $L \in k^{s\times r}$. Let W be the left orthogonal complement of $\begin{bmatrix} A \\ L \end{bmatrix}$, $\pi_r : k^{r+s} \to k^r$ the projection $\pi_r \begin{bmatrix} a_1 & \cdots & a_{r+s} \end{bmatrix} = \begin{bmatrix} a_1 & \cdots & a_r \end{bmatrix}$, and $\vec{v} \in k^r$. Then $\vec{v} \in \pi_r(W)$ if and only if $\vec{v} \in row(LA^{-1})$.*

Proof. By (3.2), $\vec{v} \in \pi_r(W)$ if and only if $\vec{v}A \in row(L)$, but $\vec{v}A \in row(L)$ if and only if $\vec{v} \in row(LA^{-1})$. □

Lemma 4.2. *Let $A \in k^{r\times r}$ be nonsingular and let $L \in k^{s\times r}$. Let $L'_0 = L$ and for each $i = 0, 1, 2, \ldots$, let $L'_{i+1} = \begin{bmatrix} L'_i \\ (L'_iA^{-1})^{(\frac{1}{p})} \end{bmatrix}$. Then for each $i = 0, 1, 2, \ldots, row(L_i) = row(L'_i)$.*

Proof. The $i = 0$ case holds since $L_0 = L'_0 = L$. Assume that for some positive integer j the statement of the proposition holds for all $i \leq j$. Let $\mathscr{B}_j$ be a basis for the left orthogonal complement of $\begin{bmatrix} A \\ L_j \end{bmatrix}$. By (4.1) and the hypothesis, $row([\mathscr{B}_j]) = row(L_jA^{-1}) = row(L'_jA^{-1})$. Therefore, $row(L_{j+1}) = row\left(\begin{bmatrix} L_j \\ [\mathscr{B}_j]^{(\frac{1}{p})} \end{bmatrix}\right) = row\left(\begin{bmatrix} L'_j \\ (L'_jA^{-1})^{(\frac{1}{p})} \end{bmatrix}\right) = row(L'_{j+1})$. □

Lemma 4.3. *Let $A \in k^{r\times r}$ be nonsingular and let $L \in k^{s\times r}$. Let $B_0 = L$ and $B_i = L^{(\frac{1}{p^i})}(A^{-1})^{(\frac{1}{p^i})} \cdots (A^{-1})^{(\frac{1}{p^2})}(A^{-1})^{(\frac{1}{p})}$ for each $i = 1, 2, 3, \ldots$. For each $i = 0, 1, 2, \ldots$, let $L''_i = \begin{bmatrix} B_0 \\ \vdots \\ B_i \end{bmatrix}$. Then for each $i = 0, 1, 2, \ldots, row(L''_i) = row(L'_i)$, where L'_i is as in (4.2).*

Proof. The $i = 0$ case holds since $L'_0 = L''_0 = L$. Assume that for some positive integer j the statement of the proposition holds for all $i \leq j$. Then $row(L'_{j+1}) = row(L'_j) + row((L'_jA^{-1})^{(\frac{1}{p})}) = row(L''_j) + row((L''_jA^{-1})^{(\frac{1}{p})}) = \sum_{i=0}^{j} row(B_i) + \sum_{i=0}^{j} row((B_iA^{-1})^{(\frac{1}{p})}) = \sum_{i=0}^{j+1} row(B_i) = row(L''_{j+1})$, since $(B_iA^{-1})^{\frac{1}{p}} = B_{i+1}$. □

Proposition 4.4. *Let $A \in k^{r\times r}$ be nonsingular and let $L \in k^{s\times r}$. Let $\widetilde{B}_0 = L$ and for each $i = 1, 2, 3, \ldots$, let $\widetilde{B}_i = L^{(p^i)}(A)^{(p^{i-1})}\cdots(A)^{(p)}(A)$. Let $\widetilde{L}_i = \begin{bmatrix}\widetilde{B}_0\\ \vdots \\ \widetilde{B}_i\end{bmatrix}$, $i \geq 0$. Then for each $i = 0, 1, 2, \ldots$, $rank(\widetilde{L}_i) = rank(L_i'')$, where L_i'' is as in (4.3).*

Proof. For each $i = 0, 1, 2, \ldots$, $\widetilde{L}_i^{(p^i)}A^{(p^{i-1})}\cdots A^{(p)}A = \begin{bmatrix}\widetilde{B}_i\\ \vdots \\ \widetilde{B}_0\end{bmatrix}$, which implies $rank(\widetilde{L}_i) = rank(L_i'')$. □

Corollary 4.5. *Let $A \in k^{r\times r}$ be nonsingular and let $L \in k^{s\times r}$. Let $r_i(A, L)$ be as defined in (3.1). Then for each $i = 0, 1, 2, \ldots$, $r_i(A, L) = rank(\widetilde{L}_i)$. In particular, if for some j, $rank(\widetilde{L}_j) = rank(\widetilde{L}_{j+1})$, then $r(A, L) = rank(\widetilde{L}_j)$.*

Proof. The first statement is immediate from (4.2), (4.3), and (4.4) and the second follows from (3.5). □

The Main Algorithm when M_g is Nonsingular 4.6. The determination of $Cl(X_g)$, as described in the previous section, when M_g is invertible involves the following simplifications. Let $n = deg(g)$, $m = \frac{n(n-1)}{2}$, and $N = m - rank(L_g)$, with L_g as described in (2.12). Calculate $\widetilde{B}_i = L_g^{(p^i)}(M_g)^{(p^{i-1})}\cdots(M_g)^{(p)}(M_g)$ for $0 \leq i \leq N$ and $\widetilde{L}_N = \begin{bmatrix}\widetilde{B}_0\\ \vdots \\ \widetilde{B}_N\end{bmatrix}$. By (3.4), (3.5), (3.10), (3.13) and (4.5), $Cl(X_g)$ is a p-group of type $(p, \ldots, p)$ of order $p^{m-rank(\widetilde{L}_N)}$.

Remark 4.7 (*Modifications to the Algorithm when M_g is Nonsingular*)**.** In (4.6) we could calculate each $\widetilde{L}_i$ together with its rank until we determine i_0, the minimal i such that $rank(\widetilde{L}_i) = rank(\widetilde{L}_{i+1})$, in which case the order of $Cl(X_g)$ will be $p^{m-rank(\widetilde{L}_{i_0})}$. We could also replace each $\widetilde{L}_i$ by its reduced row-echelon form. Lastly, note that when $g \in \mathbb{F}_p[x, y]$, then $M_g, L_g \in \mathbb{F}_p^{m\times m}$, where $\mathbb{F}_p$ is the prime subfield of k, and thus for each i, $B_i = L_g M_g^i$.

5. Examples

Example 1. Let k be an algebraically closed field of characteristic 3, $g = x + y + x^2 + y^2 + x^2y + xy^2 + x^4 + xy^3 + 2y^4$, and $X_g \subset A_k^3$ the surface defined by $z^p = g$. We have

$$M_g = \begin{bmatrix}0&2&2&1&2&1\\2&0&0&2&1&2\\0&2&2&1&2&1\\0&0&0&0&0&1\\0&0&0&0&1&2\\0&0&0&1&1&1\end{bmatrix} \quad \text{and} \quad L_g = \begin{bmatrix}0&1&1&1&0&1\end{bmatrix}.$$

Since $det(M_g) = 0$, we use the algorithm of (3.14) to calculate $Cl(X_g)$. Then $\bar{L}_0 = L_g^{(p)} = L_g$ and $A_i = M_g^{(p^i)} = M_g$ for all i. Also, following (3.15), we will replace each $\bar{L}_i$ by its reduced row-echelon form with the trivial rows deleted, which we will denote $\bar{\bar{L}}_i$. A basis of the left orthogonal complement of $\begin{bmatrix}A_0\\ \bar{L}_0\end{bmatrix}$ is $\left\{\begin{bmatrix}1&0&2&0&0&0&0\end{bmatrix}, \begin{bmatrix}1&0&0&0&0&1&1\end{bmatrix}\right\}$. Hence,

$$\bar{\bar{L}}_1 = \begin{bmatrix}1&0&0&0&0&1\\0&1&0&1&0&0\\0&0&1&0&0&1\end{bmatrix}.$$

Continuing,

$$\bar{\bar{L}}_2 = \begin{bmatrix}1&0&0&0&0&1\\0&1&0&0&1&1\\0&0&1&0&0&1\\0&0&0&1&2&2\end{bmatrix},$$

and $\bar{\bar{L}}_i = \bar{\bar{L}}_2$ for $i \geq 3$. By (3.10) the order of $Cl(X_g)$ is p^2, i.e. $Cl(X_g)$ is isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Example 2. Let k be an algebraically closed field of characteristic 3, $g = x + y + x^2 + 2xy + 2y^2 + 2xy^2 + x^4 + 2xy^3 + 2y^4$, and $X_g \subset A^3_k$ the surface defined by $z^p = g$. We have

$$M_g = \begin{bmatrix} 0 & 2 & 0 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 & 2 \\ 2 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 & 1 \end{bmatrix} \text{ and } L_g = \begin{bmatrix} 0 & 2 & 0 & 2 & 2 & 1 \end{bmatrix}.$$

Since $det(M_g) \neq 0$, we can use (4.6) to calculate $Cl(X_g)$. Then for each $i = 0, 1, 2, \ldots, \widetilde{B}_i = L_g M^i_g$ and

$$\widetilde{L}_N = \widetilde{L}_6 = \begin{bmatrix} \widetilde{B}_0 \\ \widetilde{B}_1 \\ \widetilde{B}_2 \\ \widetilde{B}_3 \\ \widetilde{B}_4 \\ \widetilde{B}_5 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 0 & 2 & 2 & 1 \\ 2 & 2 & 2 & 0 & 2 & 0 \\ 0 & 2 & 1 & 0 & 0 & 2 \\ 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 1 & 2 & 0 \\ 2 & 2 & 2 & 2 & 0 & 1 \end{bmatrix}.$$

Since $rank(L_6) = 5$, the order of $Cl(X_g)$ is p, i.e. $Cl(X_g) \cong \mathbb{Z}_p$.

Example 3. This example simply shows that the algorithm of (4.6) does not in general work if $det(M_g) = 0$. Let k and g be as in Example 1. If we were to use (4.6), then

$$\widetilde{L}_N = \widetilde{L}_6 = \begin{bmatrix} \widetilde{B}_0 \\ \widetilde{B}_1 \\ \widetilde{B}_2 \\ \widetilde{B}_3 \\ \widetilde{B}_4 \\ \widetilde{B}_5 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 2 & 2 & 2 & 1 & 1 & 2 \\ 1 & 2 & 2 & 1 & 1 & 1 \\ 1 & 0 & 0 & 2 & 1 & 2 \\ 0 & 2 & 2 & 0 & 2 & 1 \\ 1 & 1 & 1 & 1 & 0 & 2 \end{bmatrix}.$$

The rank of $\widetilde{L}_6$ is 3, but from Example 1 the order of $Cl(X_g)$ is 1 and not $p^{6-rank(\widetilde{L}_6)}$.

References

[1] P. Blass, D. Joyce, J. Lang, The divisor classes of the surface $z^{p^m} = G(x, y)$, a programmable problem, J. Algebra 100 (1986).
[2] P. Blass, J. Lang, Zariski Surfaces and Differential Equations in Characteristic $p > 0$, Dekker, New York, 1987.
[3] R. Hartshorne, Algebraic Geometry, Springer-Verlag, New York, 1977.
[4] J. Lang, C. Rogers, Applications of a new algorithm for computing class groups of Zariski Surfaces, Ulam Q. 3 (3) (1997).
[5] J. Lang, The divisor class group of the surface $z^{p^n} = G(x, y)$ over fields of characteristic $p > 0$, J. Algebra 84 (1983).
[6] J. Lang, An algorithm for calculating class groups of Zariski surfaces, preprint.
[7] P. Samuel, Lectures on unique factorization domains, in: Tata Lecture Notes, Tata Inst. Fundamental Res., Bombay, 1964.
[8] Stohr, Voloch, A formula for the Cartier operator on plane algebraic curves, J. Reine Angew. Math. 377 (1987) 49–64.